UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/588,547	06/06/2000	TARO TERAO	106408	8229

25944 7590 11/24/2004	EXAMINER
OLIFF & BERRIDGE, PLC P.O. BOX 19928 ALEXANDRIA, VA 22320	KIM, JUNG W

	ART UNIT	PAPER NUMBER
	2132	

DATE MAILED: 11/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/588,547	TERAO, TARO
	Examiner	Art Unit
	Jung W Kim	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 November 2004*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 June 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

    1.☒ Certified copies of the priority documents have been received.

    2.☐ Certified copies of the priority documents have been received in Application No. _____.

    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   The After Final amendment received on November 12, 2004 fulfills the

requirements as specified in 35 U.S.C. 1.116 and has been entered. The finality of the

previous office action is withdrawn to address the new limitations in the amended claims

which overcome the 35 U.S.C. 112, second paragraph issues raised in the subject

office action. However, this action is made Final since applicant's amendment

necessitated the new ground(s) of rejection. Applicant's period for response begins

anew with the mailing of this action.

2.   Claims 1-38 have been examined. Claims 1, 5, 7, 20, 21, 24, 25, 26, 28, 31 and

33 have been amended in the amendment filed on November 12, 2004.

Response to Amendment

3.   The 35 U.S.C. 112, second paragraph rejections to claims 1, 4, 5, 7, 8, 11-14,

20, 21, 24-26, 28 and 33 are withdrawn as the amendments overcome the rejections.

Response to Arguments

4.   The following is a response to the arguments presented by the applicant on

pages 11-18 in the amendment filed on November 12, 2004.

5.   In response to applicant's argument that the examiner's conclusion of

obviousness is based upon improper hindsight reasoning (see amendment, page 13,

last paragraph-page 14, 1st paragraph), it must be recognized that any judgment on

obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning.

But so long as it takes into account only knowledge which was within the level of

ordinary skill at the time the claimed invention was made, and does not include

knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper.

See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). In particular,

Zhang teaches strategies covering the limitations featured in the claimed inventions as

outlined below.

6.   In response to applicant's argument on page 16, 1st and 2nd full paragraphs, it is

noted that the features upon which applicant relies (i.e., processing parameters, such as

a finite Abelian group G, a prime number p, mappings pi, epsilon, and a homomorphism

g in 1st paragraph; modulo operation in 2nd paragraph) are not recited in the rejected

claim(s). Although the claims are interpreted in light of the specification, limitations from

the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26

USPQ2d 1057 (Fed. Cir. 1993).

7.   In regards to applicant's argument on page 16, third full paragraph-page 17, first

paragraph that there is no motivation to combine the teachings of Zhang with Schneier,

examiner disagrees. Schneier clearly teaches confusion and diffusion techniques to

further obscure redundancies in a message (page 237, 'Confusion and Diffusion') and

shows an example of these techniques executed by an encryption function using a

symmetric key (page 270-278, 'Description of DES').

8.   In regards to applicant's argument on page 17, 1st full paragraph that the prior art

of record does not teach calculating X(M) by applying both the one-way function H and

an encryption function E of a symmetry key to the values of u and M, examiner

disagrees. The primary reference, Zhang, covers steps for calculating X(M) by applying

a one-way function H to the values of u and M. See Zhang, col. 22, lines 37-46.

Schneier further teaches applying an encryption function having a symmetric key to a

sensitive value to hide the sensitive value. See Schneier, page 4, 'Symmetric

Algorithms'. Hence, the step of E(H(u,M)) is an obvious limitation as taught by

Schneier.

9.   In response to applicant's argument on page 17, 2nd full paragraph that due to

the nature of the inventions disclosed by the prior art of record, the combination of the

teachings of Zhang and Schneier is rendered non-obvious, the test for obviousness is

not whether the features of a secondary reference may be bodily incorporated into the

structure of the primary reference; nor is it that the claimed invention must be expressly

suggested in any one or all of the references. Rather, the test is what the combined

teachings of the references would have suggested to those of ordinary skill in the art.

See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

10.   In response to applicant's argument on page 17, 3rd full paragraph that Zhang

lacks any teaching or suggestion of using the access ticket to update values used in

authentication and so the rejections fail to show obviousness, examiner does not make

such an argument. As iterated in the previous office action and reiterated below,

Stallings teaches such a limitation.

11.   For the reasons outlined above and those listed below, the prior art of record

cover the claimed inventions.

Claim Rejections - 35 USC § 103

12.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13.   Claims 1, 2, 5-10 and 19-20 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Zhang U.S. Patent No. 6,154,541 (hereinafter Zhang) in view of

Walker et al. U.S. Patent No. 5,768,382 (hereinafter Walker) and Wolfgang et al. U.S.

Patent No. 6,625,295 (hereinafter Wolfgang).

14.   As per claim 1, Zhang covers a method for generating a one-way-function value

by applying a one-way-function to a plurality of seed values to create a hash value for a

user; these seed values and the resulting hash value cover the values u, M, and X(M)

as defined by applicant's claim 1 (see Zhang, col. 4, lines 8-25; col. 22, lines 37-46).

Although Zhang does not explicitly define combining a unique value d and a unique

value s to create the unique value u, Zhang does teach strategies of combining a

plurality of parameters to generate new parameters using the following methods as

disclosed in col. 21, line 65-col. 22, line 36 to ensure a more secure key generation

methodology:

    a.   Segmented sequences

    b.   Reassembling of fragmented/fractured numbers

    c.   Multi-seeding

    d.   Reseeding

    e.   Any combinations of the above 4.

Hence, it would be obvious to one of ordinary skill in the art at the time the invention

was made to create a unique value u from the values s and d. Motivation for such a

combination would hinder disclosure of the generated keys by attempts to

surreptitiously analyze the key generator as taught by Zhang. Further, the unique value

u is provided to a user creating the one-way function value $X(M)$.

Moreover, Zhang does not expressly disclose the unique value s to be held by a

center; however, trusted third parties are institutions that provide certified values, and

certified values are used to seed a key. For example, Walker discloses distribution of

timestamps by trusted third parties and Wolfgang teaches using a timestamp as a seed

value. See Walker, col. 28, lines 11-15; see Wolfgang, col. 7, lines 49-52. It would be

obvious to one of ordinary skill in the art at the time the invention was made for the

unique value s (the seed) to be held by a center. Motivation for such an implementation

would enable a key to be dependent on a certified seed value and as such, enable third

party authentication means of the generated key as taught by Walker and Wolfgang, and as known to one of ordinary skill in the art. Ibid.

Finally, Zhang does not disclose a token for the purpose of transferring the value u to the user. However, smart cards and other tamper-resistant enclosures are standard means of securely transferring sensitive values. On page 1, paragraph 2 of applicant's disclosure, applicant discloses such practice is a typical means. Further, examiner takes Offical Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made to use a token to transfer the value u to the user. Motivation to combine enables secure transmission of a sensitive value from a computing device to a user as known to one of ordinary skill in the art. The aforementioned covers claim 1.

15.   As per claim 2, Zhang covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, Zhang discloses means wherein the value generation unique value u is calculated by applying a one-way function G to the function generation unique value s and the unique value d (see Zhang, col. 22, lines 31-36).

16.   As per claims 5 and 6, Zhang covers a device for generating one-way function values that calculates a one-way function X dependent on a unique value d as outlined above in the claim 2 rejection under 35 U.S.C. 103(a). In addition, Zhang teaches that the steps defined above can be implemented in a smart card (see Zhang, col. 6, line 27; col. 13, line 3). The aforementioned cover claims 5 and 6.

17.   As per claims 7-9, Zhang covers a proving device for performing processing

based on a private key dependent on a message M (see col. 6, lines 19-40, especially

line 25) as outlined above in the claim 6 rejection under 35 U.S.C. 103(a). In addition,

the device covers means for performing processing based on the one-way function

X(M) (see Zhang, Figure 2, 'Crypt Unit B', and related text). The aforementioned cover

claims 7-9.

18.   As per claim 10, Zhang covers a proving device as outlined above in the claim 7

rejection under 35 U.S.C. 103(a). Zhang does not expressly disclose that the proving

device is configured as a module inside a CPU of the device. Examiner takes Official

Notice that proving devices, especially those using private keys in a cryptosystem, are

conventionally configured as a module inside a CPU of a device. It would be obvious to

one of ordinary skill in the art at the time the invention was made to configure the

proving device as a module inside a CPU of the device. Motivation for such an

implementation enables the proving device to be implemented using a processor.

19.   As per claim 19, Zhang covers a proving device as outlined above in the claim 7

rejection under 35 U.S.C. 103(a). In addition, Zhang teaches that parameters defined

by the method can be specified as variables controlling both the system and the keys

generated (see Zhang, col. 16, lines 44-45).

20.   As per claim 20, it is an apparatus claim corresponding to claim 19 and it does

not teach or define above the information claimed in claim 19. Therefore, claim 20 is

rejected under Zhang in view of Walker and Wolfgang for the same reasons set forth in

the rejections of claim 19.

21.   Claims 18, 21-30, and 33 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Zhang in view of Walker and Wolfgang, and further in view of

Stallings Cryptography and Network Security 2nd Edition (hereinafter Stallings).

22.   As per claim 18, Zhang covers a proving device as outlined above in the claim 7

rejection under 35 U.S.C. 103(a). Zhang is silent on the message M including use

conditions of the message by the method. However, use conditions specified by a

controlling message have been implemented in the analogous art of certificates. In

particular, X.509 certificates define use conditions in the extensions to the standard

parameters on the information established in the certificate (see Stallings, page 348,

bullet 'Key usage'). As such, use conditions specifying the policies under which the

values can be used or processed would be obvious to one of ordinary skill in the art at

the time the invention was made. Motivation for such an implementation would enable

a flexible means to distribute a plurality of types of messages and ensure that values

distributed are properly processed or used.

23.   As per claim 21, Zhang covers a proving device as outlined above in the claim 18

rejection under 35 U.S.C. 103(a). Furthermore, the invention disclosed by Zhang is

identified as being applicable to authentication schemes (see Zhang, col. 6, lines 19-

40), which embodiments invariable cover certification authentication schemes. As

taught by Stallings, certification authentication using public key encryption as listed in

claim 21 is a close variant of a well-known authentication method (see Stallings, page

186, 'Public-key Certificates'). Hence, it would be obvious to one of ordinary skill in the

art at the time the invention was made to implement the device disclosed by Zhang as

an authentication scheme by which the device is a right issuer by means of establishing

and issuing certificates to right recipients as taught by Stallings. Motivation for such an

implementation would enable an authentication device based on standard certificate

authentication means.

24.   As per claims 22 and 23, Zhang covers an authentication method as outlined

above in the claim 21 rejection under 35 U.S.C. 103(a). In addition, an identifier aid

indicating an authentication type and use conditions are included in the certification (see

Stallings, Figure 11.3, 'Signature'; page 348, 'Key and Policy Information').

25.   As per claims 24 and 25, they are apparatus claims corresponding to claim 21

and they do not teach or define above the information claimed in claim 21. Therefore,

claims 24 and 25 are rejected under Zhang in view of Walker, Wolfgang and Stallings

for the same reasons set forth in the rejection of claim 21.

26.   As per claims 26 and 27, Zhang covers an authentication method as outlined

above in the claim 22 rejection under 35 U.S.C. 103(a). In addition, the access ticket

specified in the applicant's claims 26 and 27 is equivalent to the issued certificate

generated by the right issuer and issued to the right recipient whereupon the rights of

the right recipient is verified by means of the certificate as claimed in claim 22. Hence,

claims 26 and 27 are covered by the invention covered by Zhang, Walker and

Wolfgang, and modified by Stallings.

27.   As per claim 28, it is an apparatus claim corresponding to claim 26 and it does

not teach or define above the information claimed in claim 26. Therefore, claim 28 is

rejected under Zhang in view of Walker, Wolfgang and Stallings for the same reasons

set forth in the rejection of claim 26.

28.   As per claims 29 and 30, Zhang covers an access ticket issuing device as

outlined in the claim 28 rejection under 35 U.S.C. 103(a). Zhang does not expressly

disclose the access ticket being calculated as a difference between the private key x

and the generated private key $X(M)$ nor as a quotient $x/X(M)$. However, as known in the

art, the difference or quotient of two values are typical mathematical operations to divine

the equality of the two values: the difference of two equal values is zero whereas the

quotient of two equal, nonzero values is one. It would be obvious to one of ordinary skill

in the art at the time the invention was made to calculate the access ticket as being

calculated as the difference or quotient of the values x and X(M). Motivation for such an

implementation allows for a simple calculation to determine if a generated value is

equivalent to a stored or received value. The aforementioned cover claims 29 and 30.

29.   As per claim 33, it is an apparatus claim corresponding to claim 26 and it does

not teach or define above the information claimed in claim 26. Therefore, claim 33 is

rejected under Zhang in view of Walker, Wolfgang and Stallings for the same reasons

set forth in the rejection of claim 26.

30.   Claims 3, 4, and 11-17 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Zhang in view of Walker and Wolfgang, and further in view of

Schneier Applied Cryptography 2nd Edition (hereinafter Schneier).

31.   As per claim 3, Zhang covers a method as outlined above in the claim 1 rejection

under 35 U.S.C. 103(a). In addition, Zhang discloses scrambling s and d to create

value u (see Zhang, col. 22, lines 31-36), but Zhang does not expressly disclose an

encryption function with a symmetric key as the scrambling operation. However as

taught by Schneier, scrambling techniques, such as diffusion and confusion, are

commonly executed by symmetric encryption algorithms (see Schneier, page 237,

'Confusion and Diffusion'; pages 270-278, Section 12.2 'Description of DES', especially

'Expansion Permutation' and 'S-Box Substitution'). It would be obvious to one of

ordinary skill in the art at the time the invention was made to apply the teaching of

Schneier to the method of Zhang. Motivation for such an implementation would utilize a

standard encryption scheme to scramble s and d to create u.

32.   As per claim 4, Zhang covers a method as outlined above in the claim 1 rejection

under 35 U.S.C. 103(a). Zhang does not expressly disclose calculating X(M) by

applying both the one-way function H and an encryption function E of a symmetric key

to the values u and M. However, as known in the art, encryption steps using symmetric

keys are efficient means to hide sensitive values (see Schneier, page 4, 'Symmetric

Algorithms'). It would be obvious to one of ordinary skill in the art at the time the

invention was made to apply the teaching of Schneier to the invention covered by

Zhang. Motivation for such an implementation would ensure that the processed value is

secured.

33.   As per claims 11-17, Zhang covers a proving device as outlined above in the

claim 7 rejection under 35 U.S.C. 103(a). In addition, the processing steps by the

proving device as listed in dependent claims 11-17 are generic implementations of well-

established cryptosystems as taught by Schneier. In summary, claims 11 and 12 are

processing means to implement any type of verification scheme using a challenge

variable such as a DSA signature algorithm (see Schneier, pages 486-487, 'Description

of DSA', where H(m) is the challenge variable); claims 13-14 are processing means to

implement authentication schemes having commitment values such as the Schnorr

authentication (see Schneier, page 511, 'Authentication Protocol', where x is the

commitment); claims 15 and 17, read on encryption schemes using multiplication,

power operations, and modular arithmetic, including DSA signature and Schnorr

authentication schemes as listed earlier; and finally, claim 16 reads on operations using

elliptic curve cryptosystems (see Schneier, page 480, Section 19.8). It would be

obvious to one of ordinary skill in the art at the time the invention was made to perform

the processing based on standard cryptosystems. Motivation for such implementations

ensures that the proving device is derived from proven cryptosystems.

34.   Claims 31-32 and 34-38 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Zhang in view of Walker, Wolfgang, Schneier, and Stallings.

35.   As per claims 31 and 32, Zhang covers an access ticket issuing device as

outlined above in the claim 28 rejection under 35 U.S.C. 103(a). Although Zhang does

not expressly disclose combining two values as defined in claims 31 and 32, this type of

operation on two variables is typical especially when the two values are of differing

sizes. An example of this strategy is found in DES. A plaintext p is broken into 64-bit

segments (p_1, p_2, ..., p_n) and each segment is operated on by a 56 bit key k (see

Schneier, pages 270-278, Section 12.2, 'Description of DES'). Furthermore, the

resulting value has a standard size corresponding to the number of segments and the

processed segment length, which is essential so that resulting values can be

reconfigured into alternative but consistent formats. It would be obvious to one of

ordinary skill in the art at the time the invention was made to combine two values by

segmenting one value and applying each segmented value to the other value.

Motivation for such an implementation enables two different formatted values to be

combined where each part of the resulting value is dependent on both of the two values.

36.   As per claims 34-38, Zhang covers an authentication device as outlined above in

the claim 33 rejection under 35 U.S.C. 103(a). Although Zhang does not expressly

disclose using the access ticket to update values used in authentication, these steps are

obvious implementations for the following reasons: an access ticket expressed as a

difference or a quotient of private key x and value $X(M)$ are obvious constructions to

show equality/inequality of two values as argued above in the claim 29 and 30

rejections, and further, the updates in claims 34-38 are obvious means to communicate

the resulting discrepancy between x and $X(M)$ to an authenticator in the authentication

schemes as summarized by Schneier and listed above. As defined in the applicant's

Specification (see expressions 65, 67, and 69 on page 48), the update procedure is

defined by applying the following types of operations: $z = z + z^*(x - X(M))$, $z =$

$z^\wedge(x/X(M))$, or $z = z/(x/X(M))$, wherein the z variable is a challenge or response value

defined in a step of a conventional authentication scheme. In these cases, z remains

the same if $x == X(M)$, and is updated to a different value if $x != X(M)$. Furthermore, as

taught by Stallings, challenge or response approaches used in authentication methods

typically comprise steps of submitting a value by a sender wherein the receiver is

required to return the same value back to the sender (see Stallings, page 304, bullet

'Challenge/response'). Hence, the steps of claims 34-38 are simple variations of this

theme. It would be obvious to one of ordinary skill in the art at the time the invention

was made to update challenge or response values in step(s) of implemented

authentication schemes to determine if a generated value is equivalent to a stored or

received value and thus determine authentication. Motivation for such an

implementation would use simple update functions to determine if authentication has

succeeded or failed. The aforementioned cover claims 34-38.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
November 18, 2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100